Chapter 78
Improving Dependability of Robotics Systems

Nidhal Mahmud
University of Hull, UK

ABSTRACT

The use of robotics systems is increasingly widespread and spans a variety of application areas. From healthcare to manufacturing to space missions, these systems are typically conceived to perform dangerous or critical tasks. The nature of such tasks (e.g., surgery operations or radioactive waste clean-up) places high demands on the dependability of robotics systems. Fault tree analysis is among the most often used dependability assessment techniques in various domains of robotics. However, fault tree analysis of cost-effective fault tolerant robotics systems requires compositional synthesis of fault trees extended with the expressive power to allow analyzing the sequential dependencies among the components. Thereafter, a relevant experience from the automotive domain is presented. This consists mainly of a suitable synthesis approach that computes expressions of global failure conditions from the dysfunctional behavior local to the components. The benefits of the approach to dependability analysis of robotics architectures are highlighted by using a fault-tolerant example system.

INTRODUCTION

The use of robotics systems is widespread and spans a variety of application areas. From healthcare, to manufacturing, to nuclear power plants, to space missions, these systems are typically conceived to perform difficult, dangerous or critical tasks. The nature of such tasks (e.g., surgery operations, radio-active waste clean-up or space mining) places high demands on the dependability of robotics systems.

The preoccupations in the dependability of robotics systems are not new. Fault Tree Analysis (FTA; Vesely, 1981) and Failure Modes and Effects Analysis (FMEA; IEEE Std.352, 1987) are among the most often used techniques in various domains of robotics. For instance, Visinsky, Walker, and Cavallaro (1993) describe the use of FTA for robots operating in remote and hazardous environments. Other fields of application include industrial robots like in Karbasian, Mehr, and Agharajabi (2012), and modular and swarm robots like in Murray, Liu, Winfield, Timmis, and Tyrrell (2012).

DOI: 10.4018/978-1-5225-7368-5.ch078

The widespread use of FTA in the dependability assessment of complex systems is mainly due to the flexibility and ease of use of the fault trees. These are static (i.e., 'pure' Boolean) models, and therefore enable the use of efficient Boolean calculus in the elimination of component failures that are irrelevant to the total failure of the system. This logical reduction (known as qualitative analysis) simplifies the process to produce overall probabilities of system hazards (i.e., quantitative analysis). Nevertheless, such convenience comes with the loss of the significance of the sequencing of failure events—i.e., the dynamic features often exhibited by modern systems cannot be captured by combinatorial models like this type of fault trees.

Robotics systems are certainly not an exception when it comes to sequence-dependent failures. For example, preclusion of the dynamic aspects due to the use of static fault trees in the analysis of modular robotic systems is clearly noted in Murray et al. (2012). To overcome such drawback, an alternative can be the utilization of fault trees that are extended with capabilities to capture the dynamic features. A well-known example is the Dynamic Fault Tree (DFT) approach (Dugan, Bavuso, & Boyd, 1992). This method was primarily conceived for quantitative analysis, which is often state-based (i.e., Markov analysis which is based on state transition diagrams [Markov models] is the DFT most prominent solving technique). That is, the full power of the Boolean methods was sacrificed here, especially when it comes to analyzing the dynamic parts of the system at the level of the fault tree (i.e., reducing the DFT).

Theoretically, some later research efforts have provided workarounds to the question of FTA with dynamic aspects. To deal with it, a technique which is relevant to this article consists of extending the Boolean methods with temporal logic calculus. In this connection, a set of temporal laws that enable qualitative analysis of fault trees extended with dynamic features can be found in Walker and Papadopoulos (2009). In the same vein, the algebraic formalism in Merle, Roussel, Lesage, and Bobbio (2010) proposes formal descriptions of dynamic behaviors and provides proofs of a number of theorems useful for the qualitative analysis of this type of fault trees. The latter approach also deals with the corresponding probabilistic algebraic analysis.

In practice, automation of such advanced FTA as part of integrated dependability and systems engineering processes requires an automated generation and synthesis of these fault trees from failure behavioral models that are linked to the system specifications. The work in Mahmud, Walker, and Papadopoulos (2012) describes a suitable approach to generating and synthesizing fault trees that preserve the significance of the event-order from hierarchical models. Application areas for this approach include the automotive domain (Chen, Mahmud, Walker, Feng, Lönn, & Papadopoulos, 2013). More details about integration in an extended FTA through a Model-Based development process can be found in Kolagari et al. (2015).

In this article, emphasis is put on the significance of the sequencing of failure events and its implications in dependability analysis of robotics systems using FTA. Accordingly, a suitable technique for automated generation and synthesis of extended fault trees from system models is presented. Furthermore, we outline a novel approach to automated reduction of these fault trees. The article is structured as follows: the background section provides a literature review and highlights the relevant approaches to generating and synthesizing fault trees from systems models. The next section outlines an algorithm for the logical reduction of fault tree algebraic expressions that are extended with temporal semantics. Then, an advanced fault tree synthesis approach is presented in the following section. Finally, we present some future research directions, then we conclude.